INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

BIOMETRIC IDENTITY – FROM COLONIAL FINGERPRINTING TO AADHAR SYSTEM

AUTHORED BY - SHAIKH MASIRA YUSUF
FYBALLB, Mumbai University

Abstract

This research paper examines how biometric identity has developed in India. Starting from the methods used in British colonial period to the present day Aadhar system. Biometric use special physical features, such as fingerprint and the pattern in your eye, to recognize and identify people. Although these tools help's make government service better but at the same time it also bring big risk to privacy and human right, the study begins by looking at the history of fingerprint during the colonial era. The first fingerprinting methods started in Bengal with British official such as William James Herschel and Edward Henry were involved in beginning of this practice. However, during this time biometric were only used for police work and watching people over. The aim was to track and manage the population instead of offering social benefit. The attention then moves to the Aadhar system, which is handled by UIDAI. The paper describes how Aadhar changes the way people prove their identity by creating a central system that stored fingerprint and iris scan data, making is easer for citizen to open bank account and receive government benefit. The Indian constitution's Article 21 supports this system as a way to help with development, but at the same time the research also says that law needs to protect a person's privacy and respect for their dignity. This research paper also examines how biometric data is being used wrongly it deals with issue such as data leaks, government monitoring and exclusion where poor people don't get food because their fingerprint doesn't work properly due to being too old or rough work the paper also suggest solution like better laws to protect personal data and harsh punishment for data leaks. The study also says that although biometrics are strong tools, India needs to make sure that technology doesn't break basic human right.

Key points include: Biometric, Aadhar, privacy, Colonial history and Government.

ISSN: 2582-6433

Objectives:

- To study the origin of biometric identity in colonial India: how fingerprint started in Bengal under British rule.
- To analyse the Aadhar system in modern India: how current biometric system works
- To examine the misuse of biometric data: to identify the risk associated with biometric identity.
- To study constitutional and legal protection in India: to understand how the Indian constitution, specifically Article 21, protects a citizen's right to privacy and dignity in the digital age.

Methodology:

- This paper uses a qualitative and doctrinal research method.
- the study is based on secondary research: reviewing historical archives of colonial fingerprinting and official UIDAI reports on Aadhar.
- legal analysis: studying the Aadhar Act and Supreme Court judgment regarding Article 21 and the right to privacy
- Comparative study: Analysing the biometric policies of the UK and China to provide a global perspective on India's system
- Data collection: gathering information from government websites, academic journals, and news report focused on data security and welfare exclusion.

Introduction

The story of identity in India. It started with how people proves who they are has completely changed over time. In the past, people use to prove who they were by showing a piece of paper or a plastic card. But today identity is about you – your actual body and appearance, biometric identity means a system that identifies people by looking at their special body characteristics. In India, this idea has been around for along time. It began during British rule with simple ink and paper fingerprint and now has developed into Aadhar, one of the biggest and most advanced digital identification in the world.

What is Biometric Identity? -

Biometric identity is a method of recognizing a person based on unique features of their body. You can't forget your biometric like you can forget a password or pin, and you can't lose them

 ISSN: 2582-6433

like you can lose an ID card.

Fingerprint: fingerprint is the most common type of biometric. Every person ha a small pattern made of rigids and valleys on their fingertips. Even identical twins have different fingerprint to figure out how they work let's look into the three main types.

[1]1. Loops: lines that blend back to themselves

2. Whorls: circle like patterns

3. Arches: looks like wave



Back in the days people used link to create these prints on paper. Today, we use electronic scanners that take a digital photo of these lines and convert them into a unique code. Scientists including Francis Galton proves that these prints are "permanent" which means they stay the same from the time someone is born until the day they are passed away.

Iris Scan: The iris is the coloured part of your eye around pupil it has really complicated patterns that are even more special than fingerprint. To use this, a special camera captures a clear picture of your eyes it doesn't hit you eyes and moves really quickly.

How it was used: At the beginning it was used b y policed to catch criminals. If someone does something wrong and leaves a fingerprint the police can check their data base to find out who it belongs to. It was also used for "prisoners" and retired worker to ensure correct person is getting their pension.

How Police Official's use Biometric to Track Criminals Today

Modern Criminal Data Collection: How the colonial system evolved

To understand how India keeps track of Criminals today, we need to examine how an old British law from 100 years ago was entirely taken apart and replaced with modern digital system. The main ideal is still the same- using the human body to catch criminals but the size, technology, and legal authority have increased a lot.

1.1 The Legal Shift: Out with the Old In with New

For more than a hundred years, the police relied on an old law from the colonial era known

[1] Aratek : What is Fingerprint https://www.aratek.co/news/what-is-a-fingerprint Dec 31 2022.

ISSN: 2582-6433

as *The Identification of Prisoners Act,1920*. This law was very limited. The police were only allowed to collect basic ink fingerprint, footprint, and photographs, and they could only do this for people who had been involved in serious crimes.

On August 4, 2022, the Indian Parliament introduced a stronger new Law named as The Criminal (Identification) Act, 2022. This new law has changed the rules entirely:

What the Police can Collect [2](Section 2 (1)(b)): The la has broadened the meaning of "measurement." Now, police can collect more than fingerprint. They have the have the right to ask for iris scan (eye scan), retina scan, palm scan, physical signature, and a sample of your handwriting. They can also gather biological samples such as DNA, blood, and hair.

Who can be Targeted [3](Section 3): According to the previous British law, minor offenders were protected from being tracked through biometrics. According to the new law of 2022, police are allowed to collect biometric from anyone who is arrested for any crime or even if they are held for preventive reason.

An Important Exception: To prevent serious abuse, the law states that police cannot force someone to provide biological samples such as DNA, or blood, unless they have been arrested for a serious offence that carries a punishment of 7 years or more in prison, or for a crime against a women or a child. But regular biometrics, such as fingerprint and iris scan can be collected from anyone who has been arrested for any reason.

1.2 The Technical Shift: From Paper cards to the NAFIS Cloud Network

During the colonial times, if u get arrested, the police would press your ink-stained fingers onto a paper card. These cards were kept in a filing cabinet nearby. If someone did something illegal in one state, the police couldn't connect their fingerprints

Today those old paper files have been swapped out by two larges digital system:

1. CCTN (Crime and Criminal Tracking Network & System): This is a national digital network that connects more than [4]15,000 police station through India. It turns whole criminal history into a digital system- from the first police report to the last court decision so it can be seen across different states.
2. NAFIS (National Automated Fingerprint Identification System): The NAFIS, is controlled by National Crime Record Bureau (NCRB) located in new Delhi. Is a powerful computer system that stores biometric data, specifically fingerprint. A police

[2] The Criminal Procedure (Identification) Act, 2022, § 2(1)(b), No. 11, Act of Parliament,2022 India,
[3] The Criminal Procedure (Identification) Act, 2022, § 3 No. 11, Act of Parliament, 2022 India.
[4] Crime and Criminal Tracking Network and System (CCTNS), Vikaspedia: Digital Governance Portal Jan 4 2024.

 ISSN: 2582-6433

officer uses a digital glass scanner to scan suspect's finger instead of using ink. In just a few seconds, the print is sent to a main data base that contains more than [5]1 crore criminal record.

1.3 The Algorithmic Shift: The 10 Digit National Fingerprint Number (NFN):

The biggest improvement today is how technology helps keep track of criminals automatically, in the British system, specialist had to use magnifying glasses to manually compare fingerprint.

Today its done right away by a computer program that uses a 10-Digit National Fingerprint Number (NFN)

1. When a suspect's fingerprint are added to NAFIS, the system looks at special patterns on the fingers.
2. If the system has not encountered this person before, it generates a special 10-Digit Code. The first two digits represents the state from where they were caught, and the next eight digits are their unique identification.
3. This NFN will serve as a lifelong Digital Criminal I'D, if the criminal gets arrested by using a false name in Delhi, but their fingerprint were uploaded years earlier in Mumbai, the NAFIS scanner will quickly identify their real name and show their complete criminal history to the officer in just few seconds.

1.4 The Time Line Shift: The 75 years storage rule (Section 4)

The last big change Is about how long the government can hold onto your information, paper records can wear out over time, but digital can last indefinitely.

According to the Section 4 of the 2022 Act, the NCRB has the legal right to keep, share maintain a person's biometrics, iris scan, and DNA information in their electronic records for [6]75 years from the date it is collected.

This means that if someone get into the police database, they will likely be tracked digitally by the government for almost their entire life. Data is only deleted right away if a court fully clears the person and they don't have any past criminal records.

[5] National Automated Fingerprint Identification System (NAFIS) Dec 4 2024/
[6] The Criminal Procedure (Identification) Act, 20222, § 4, No.11, Acts of Parliament, 2022 Available at PRS Legislative Research https://prsindia.org/files/bills_acts/bills_parliament/2022/The%20Criminal%20Procedure%20(Identification)%20Bill,%202022.pdf

ISSN: 2582-6433

Its Importance in Modern Governance-

In a big country like India, the government has to offer services to more than 1.4 billion people. Biometrics are really important for how the government runs the country. In the past, one of the main issue the government faced was “leakage” this means that money or food that was supposed to go to poor people got stolen by people who used fake names or made up identities. With modern governance system, this problem was solved because they make sure each person is unique. Because biometrics are connected to a real person’s body, its not possible for someone to have to different online identities. This make sure that the person at a ration shop or at bank is really who they claim to be.

Biometrics also helps with Direct Benefit Transfer (DBT). Instead of money going through many people’s hands where it might be taken, the government can send the money straight into someone’s bank account and they can confirm their identity using their fingerprint and iris scan. It also means that people don’t always have to be physically present; for example, older adults can use a smartphone and just press their thumb to sign a “Digital Life Certificate” so they can continue getting their pension. This helps the government work better, be more open and saves a lot of money that would normally be wasted due to corruption. In simple terms, it has made the human body into a secure and universal key for getting involved in public matters, so that no one is left out because they lost a physical document.

India’s Journey from British Era to Aadhar-

India has a very interesting history with biometrics. Many people are not aware that the modern use of fingerprint started in India during colonial era. In the 1850s a British officer named William Herschel in Bengal began asking people to leave their handprint on contracts. He understood that even though people can say untrue things, they can’t alter the mark their hands leave. Later another official named Edward Henry worked with two Indian expert, Azizul Haque and Hem Chandra Bose, to develop a mathematical system for organizing millions of fingerprint. This is called The Henry Classification System, in 1897, they started the world’s first Fingerprint Bureau in Calcutta, which is now Kolkata.

Today, in the present time, India has taken that old concept and developed it into Aadhar while the British used fingerprint to track people, the Indian government made Aadhar to assist people. Aadhar was started in 2009 with the goal of providing a legal identity to million of people who don’t have birth certificates or school documents. It used fingerprint and iris scan together, making the system very hard to fool. It changed India from using old, dusty paper records to the digital age, making India a world leader in how a country recognizes its citizen.

ISSN: 2582-6433

Colonial Fingerprinting Era

the history of using biometric identification in India didn't start with todays advanced technology; it actually began in the middle of 1800s during the time when British controlled India. Unlike modern systems that focus on helping people, the British used fingerprinting as a specific tool for police work, managing people, and keeping track of them.

The Origin-

the beginning of using fingerprint started with William James Herschel, a British officer working in the Bengal Civil Service in the late 1850s in India. While working in the Jungipoor and Nadia Districts, Herschel had a issue he couldn't check the identities of local contractors or prisoners. Signatures were not always real or genuine to fix this problem, Herschel started asking people to put their handprint and later fingerprint, on legal documents. He understood that each person's biological mark was one of kind and never changed. This was the first time biological trait was used by the colonial government to stop fraud and make sure people were really who they said they were.

Edward Henry and The Classification System-

While Herschel showed that fingerprints were unique, the government had a new problem like how to sort through and find thousands of fingerprints. In the late 1890s, Edward Henry who was the Inspector General of Police in Bengal, was very important in this work. He worked with two Indians Sub-Inspector Azizul Haque and Hem Chandra Bose, and together they created a special way of to sort fingerprint by looking at their shape this system came to be called The Henry Classification System. Because of this important discovery the world's first Fingerprint Bureau was discovered in 1897. This system let the police quickly compare a fingerprint found out a crime scene with a specific person's print just in a few minutes.

A Tool to Control-

It's important to remember that during the colonial period, fingerprint was ot used to improve social welfare or assist the public. Its main job was to help with controlling and managing the state. The British used these biometrics data to track and record people from "Criminal Tribes", those who were imprisoned and individual who worked as laborers. It was a system that controlled everything from top down, means to keep of people the rulers didn't trust. By connecting a person's real body to criminal file, the British set up a strong way of watching people, making it very hard for anyone to stay hidden from government. This legacy of using

ISSN: 2582-6433

biometrics as a tool for state power set the stage for the identification of India uses today.

Aadhar System in India – The modern Identity Revolution

Here we will look at how India moved from old colonial identity system to create the world's biggest biometric system – Aadhar.

Unique Identification System of India (UIDAI):

The Aadhar project was started by Unique Identification System of India (UIDAI). UIDAI is a government body that handle everything related to Aadhar. It was setup in January 2009 by the Planning Commission of India. The aim was to tackle the main issue such as millions of Indians didn't have proper identification, which made it harder from them to show who they were in order to receive government assistance. To make it official, the government later passed the Aadhar Act in 2016, which gave the UIDAI the legal authority to handled identity management. UIDAI didn't just gave out cards; it also takes care of technology that protects your data and make sure that when you use your fingerprint at a store or bank the system can instantly recognize you. It was made to change how "identity" is handled into a digital service that works everywhere in the country.

The Success Behind Aadhar-

Nandan Niekani, who co-founded the big tech company Infosys, is the main reason behind Aadhar success. In 2009, he was asked by Indian government to be the first chairman of the UIDAI. Nilekani brought a mindset that focused on using technology first when working with the government. He didn't want Aadhar to be just another piece of paper or he could copy o forgotten. Instead, he saw it as a digital platform. Under his leadership, the project progressed faster than ever before, signing of hundreds of millions of people in just few years his main goal was to build a system that was "Online and Authenticable," which means your identity could be checked quickly over the internet, something that had never been done on this large scale before.

Fingerprint and Iris as a Central Database-

Aadhar is special because it uses multiple types of biometric data. This means that it doesn't depend on just one thing. When someone signs up, the system takes all ten fingerprints of their hand and scan both of their irises, plus a picture. This level of detail makes sure that each person has a unique Aadhar number and no one can have the same or related number twice. All of this

ISSN: 2582-6433

information is kept in a Central Identities Data Repository (CIDR), which is one of the biggest and safest digital storage places in the world. Since the data is placed in stored in one place, a person can check their identity in a village in Bihar or in a big city like Mumbai using the same information database. This rule, which says one person can only have one ID, was made to stop people from using fake names to take government resources.

Use of Aadhar System-

Aadhar main purpose was to serve as a Direct Benefit Transfer (DBT) to0ol. It was intended to be used for welfare programs, banking services, and as a form of identification. Before Aadhar, government money meant for poor people, like subsides for cooking gas or rice, often ended up in the hands of middleman. The money is sent straight into a bank account that is connected to an Aadhar number. In banking, it made "know Your Customer" (KYC) really easy: people who never had a passport or driving license could open a bank account just by a using their thumbprint. Besides money, it also acts as a general I'D for things like getting SIM card, setting up a gas connection, or even accessing a digital locker or storing document. It changed a person's body in their most dependable "document," so even the poorest people are no longer hidden from the government.

The main point is that Aadhar serves as both a developmental tool and an identity system. The key message is that Aadhar was created to do more than just provide service. The colonial system was designed to keep track of people, but Aadhar was created to bring people into the system. It considers identity as a basic "right" that lets a citizen participate in in the digital economy. India made a system where a real person is linked with a 12 - digit number. This helps the government provide services and support to the right person at the right time, making sure nothing is lost or given to the wrong person.

1.[7]Justice K.S Puttaswamy v. Union of India (2017) – The Right to Privacy. This case is often called as "Privacy Reference." It was heard by 9 judge bench to settle a massive debate: Does a person "own" their body and data, or does the State?

Retired Justice Puttaswamy argued that the Aadhar project was being build without a safety net. The Government's defence was shocked was shocking at the time they argued that the Indian Constitution did not explicitly grant a "right to privacy." The court ruled that Privacy is a Fundamental Right under Article 21. They defined privacy as "the right to be left alone."

[7] Justice K.S Puttaswamy v. Union of India (2017) 10 SCC 1
Page: 509 para no.: d 325.

ISSN: 2582-6433

They established that the Triple Test: for the State to take your data, there must be a Law, a Need, and Proportionality means they should not collect data more than necessary. This judgment is the "Turning point" it proves that the era of Colonial Surveillance where the State could take your print without question is legally over. By declaring privacy as Fundamental Right, the law has officially has moved from treating citizen as "subjects to be watched" to "individual with right".

2.[8] Justice K.S Puttaswamy v. Union of India (2018) – The Aadhar Case. A 5 judge bench sat down to see if the actual Aadhar Act passed the "Triple Test."

Petitioners argued that Aadhar was a "giant glass house" where the state could see everything a citizen does. They challenged how the law was passed as a Money Bill. The court took the middle path. They upheld Aadhar for government welfare like PDS ration because it helps the poor get their due. However, they struck down Section 57, which allowed private companies to give Aadhar for an exam or a citizen to link it to SIM card was "disproportionate." This focus on the Evolution of Identity. It shows that while we accept biometrics for development like getting food, money to the poor, the law rejects it for Control letting private companies or the state track your every phone call or bank transaction.

Misuse of Biometric Identity in India

The shift from using paper document to show who you are to single system that uses biometric data has made the system more prone to weakness. In physical paper system, if an I'D card is stolen or becomes compromised it can be cancelled, revoked, and a new one can be issued. However, biometric data like fingerprint and iris scan includes biological feature that cannot be changed and are connected directly to the person's body. Once these biological patterns are shared, copied, or used incorrectly, they become unsafe and can't be fixed for the rest of the person's life. This ongoing weakness serves as the foundation for numerous serious violation of rights.

1. <u>Privacy Violations</u>

   A serious privacy problem happens when someone's private information, like medical history or personal details, is shared with public without them giving clear and thoughtful permission. The system failed because when the Aadhar program started

[8] Justice K.S Puttaswamyh v. Union of India (2019) 1 SCC 1
Page: 442 para no.: 447, 448.

ISSN: 2582-6433

quickly, many governmental offices hurried to connect citizen's data with their services without setting up proper security measures like standard encryption rules. [9]The administrative mistake lead to many "publishing leaks." More than 200 central and state government websites accidentally made large, unencrypted directories available online, exposing the names, home addresses, bank account numbers, and matching Aadhar number of millions of citizen on public web portals. Because Aadhar serves as a main key that connects various services, these leaks let bad people easily gather information to steal identities a6nd6 commit very targeted financial fraud, breaking the basic right to privacy.

2. Data Breach

A data breach happens when someone not allowed to access it gets into a digital database and views private information that was meant to be kept secure.

The Unique Identification Authority of India (UIDAI) keeps the biometric data and personal information of more than 1.3 billion people in one main database called the Central Identities Data Repository (CIDR). In computer security, keeping all data in one stop is called "honey pot." This setup is very appealing and easy to attack for hackers, cybercrimes, and data brokers.

[10]In January 2018. The Tribune published a big investigation that showed people on Whatsapp were offering full access to the whole citizen database for just ₹500 through a digital wallet. This showed that centralized system are very weak and can be easily break down. If a credit card database is hacked, the bank can replace the card number. But if the CIDR is compromised, people can't change their fingerprint or eyes, making the security risk permanent and unchanged.

3. Surveillance by State

During British Colonial time, people used manual fingerprint to keep track and control groups that were considered criminals. A modern centralized digital biometric system enables the state to conduct passive, automated mass surveillance over the entire population.

The way failure happens is through mass surveillance in the digital age, which uses

[9] The Financial Express – UIDAI admits 210 government websites made Aadhar details public Article published: November 20, 2017.

[10] Rachna Khaira, Rs 500, 10 minutes, and you have the Access to Billion Aadhar Details, The Tribune India Jan 04 (2018)

ISSN: 2582-6433

metadata and track transaction. Each time a person uses their Aadhar card to prove who they are for example, to get a mobile SIM, open a bank account, arrange travel, or get a government benefits the system sends a request to check their identity against the main database. The system keeps a record of precise time, date, place and type of activity in an authenticating log. By considering these digital logs, the state can track a citizen's everyday activities, connections, and financial behaviour without needing to monitor them in person.

This allows detailed surveillance of people's lives from distance. This ongoing watching makes people afraid to speak freely and challenge the government. When people know their biological traits are being tracked by a government database, they tent to self-censor and stay away from political activities like protest or rallies, similar to how population were controlled during colonial period.

4. Exclusion (Fingerprint Mismatch)

Technological error occurs when a system's mathematical algorithm fail to account for the real world condition the working class body. Their effectively denying vulnerable individual their fundamental constitution rights.

The reason biometric scanners fail is because they need a clear, high contrast physical print to confirm someone's identity. Many millions of people who works in farming, building, and really elderly people have rough, dry or scarred skin on their finger from years of rough work. This is called biometric wear and tear. When these people put their fingers on scanner to get their required, government supported food grains through Public Distribution System (PDS), the machine says that fingerprint doesn't match, which is called fingerprint rejection. Because the government required Aadhar authentication to get food these technical issues have prevented poorest families from accessing the welfare system.

5. Unauthorized Use by Private Companies

When private companies use public system that are required by the government to collect biometric data, and they I it without permission to gather information for their own benefit and make more money.

In the original version of law the government added section 57 of the Aadhar Act, which allowed private companies to use Aadhar biometric identification for checking someone's identity. By using this opportunity, private telecom companies, banks, and

ISSN: 2582-6433

digital loan apps pushed customers to have their biometric data scanned in order to get simple, non-government services like buying a mobile phone.

The consequences for citizen were significant. Private companies used this low-cost, public verification system to quickly gather and compare personal information creating comprehensive profit of consumer's buying behaviour without the individuals fully understanding or agreeing to it. Although Supreme Court later remove section 57 to limit this private overreach, digital fintech platform and private companies still use the legal gaps to gather biometric data, turning citizen's personal identities into a tool for corporation profit.

The main point is that biometric system can cause major violation of people's rights. When a state creates a large, centralized database with the biological information of all its citizen, it creates a powerful system for controlling the population. Biometric can easily break important rights protected by the constitution, whether because of technical problems like system not recognizing to a person's fingerprint, security issue like hackers getting into database, or how policies are designed, such as tracking people's activities or profiling them based on their corporate data. This digital identity system can end up doing the same kind of population control used in the past during colonial times.

Biometric Governance Across the Borders

To truly grasp India's biometric system, it's important to look at how it compares to other system around the world. Biometric governance usually lies somewhere between two main option: One where people have complete privacy and other where government the has total control.

The United Kingdom: A Right-Based, Minimalist System.

The United Kingdom operates a right-based system that emphasizes individual privacy and places strict limits to how the government can gather and utilize biometric data In United Kingdom, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 classify biometric data as "special category data" under law. This means it gives the strongest level of protection. Unless they have very strict legal permission or you give them clear and free consent, the government or private companies can't gather or use your biometric information.

The United Kingdom does not maintain a single biometric database that includes information

ISSN: 2582-6433

of all its citizens. In fact, in 2010, the United Kingdom government passes the Identity Document Bill, which fully cancelled and destroyed its planned National Identity Card program and shut down its main database to safeguard people's civil right. In the United Kingdom, biometric are mainly used in specific areas like criminal justice and temporary immigration control. They aren't connect to regular everyday life, money transaction, or public service.

China: An Intensive, State Controlled Surveillance System.

On the other side, China uses a government-run approach where biometric technology is heavily used with in the government system to influence society, manage law enforcement and maintain complete control over people's lives.

China has created the biggest, network of facial recognition system in the world, this system is supported by government project such as "Skynet" and "Sharp Eyes," There are million of high-quality smart CCTV cameras that use artificial intelligence. These cameras are places in both big cities and small villages. These cameras don't just take videos they also use facial recognition and behaviour analysis to quickly spot people on the street as they walk.

In China, biometric tracking is deeply integrated into everyday life and is closely connected to the country's wider government system, including the Social Credit System. Your face information is connected to your phone account, online voice use, and payment apps. If the state's algorithms identify "untrustworthy" behaviour, like jaywalking, not paying debts, or taking part in dissent, the system can immediately limit your biometric access. This can stop you from getting on high-speed trains, purchasing plane ticket or entering public building. This technology is used directly to enforce political rules and watch over large groups of people.

India's Middle Position: Balancing Development and Rights

India is in a complicated middle place of this spectrum. It doesn't have the strong legal protection focused on rights that the United Kingdom has, and it doesn't use complete, unrestricted surveillance like China does.

While United Kingdom stopped using it's national Identity System to keep civil liberties, India created Aadhar. India's main data privacy law, the Digital Personal Data Protection Act, is still being developed and includes wide exemptions for government agencies. This means that Indian Citizen don't have the same kind of protection from government data collection as United Kingdom citizen's have under the GDPR.

India is not as strict as China's system, but still isn't the same as China's way of governing. India is a constitutional democracy. The Indian court system serves as a strong protector against

ISSN: 2582-6433

excessive government power. This was confirmed in landmark puttaswamy judgment, where the Supreme Court of India recognized privacy as a Fundamental Right under Article 21, stopped private companies from asking for Aadhar information, and set up legal "proportionality" tests that the government must meet before collecting personal data from citizen. India has strong biometric technology, but its democratic system and active judiciary stop it from becoming a fully controlled AI-based surveillance state like China.

Prevention of Misuse: Balancing Technology & Fundamental Right

To make sure India's biometric program doesn't turn into a system that watches too closely, there needs to be a "Three-Pillar" approach Legal, Administrative, and technical.

1. Strong Data Protection Law (The Legal Shield)

   The law should serve as a strong protective shield, acting as a barrier between a citizen's personal life and the power of the state or corporations. This legal framework ensures that individual's private information is safeguarded from being misused by the powerful entities.

   With the passing of the Digital Personal Data Protection (DPDP) Act 2023, India now has a legal system in place that regulates personal data. This law puts biometric data into specific group of personal information. It confirms that data should be processed only for a "Lawful purpose" and introduces the idea of Data Fiduciaries-Entities, such as the government or banks, that are legally responsible for the "duty of care" regarding your data.

   It shifts the responsibility of security from the individual to the organisation. If a government department loses data, they can no longer say they are protected by administrative immunity. They become legally responsible for any harm caused, such as identity theft or improper surveillance.

2. Doctrine of Informed Consent. (The Power of Choice)

   The Doctrine of Information Consent, also known as The Power of Choice, emphasizes that consent is the foundation of privacy, consent is the heartbeat of privacy, ensuring that individual have the right to make informed decisions about their personal information. It has to be a deliberate choice, not something that's required without being noticed.

   Under the Aadhar (Amendment) Act, 2019, the concept of the law. This means that an

ISSN: 2582-6433

agency has to clearly tell you exactly what data they are collecting and the reason behind it. Important thing is, it introduced Voluntary Enrolment: the law now says that no citizen can be stopped from getting a service, like bank account or a SIM card, just because they don't want to use Aadhar, they need to be provided with an "alternate and viable means of identification," like a passport or Voter ID. It prevents the "State of Exception" where a person is forced to choose between their privacy and their survival, such as having to choose between food and money.

3. Data Minimization & Limiting Use (The "Silo" Architecture)

   The government should not know more about your life than is necessary for the specific service you are using.

   This rule makes sure that information stays within the Silos. For example if you use Aadhar for a food subsidy, the database should not connect that information with your travel history or your hospital records. The Puttaswamy 2018 judgment strictly struck down section 57 of Aadhar Act, which allowed private companies to use the database. This effectively prevented private tech giants from engaging in data crawling.

   It is important because it stops the formation of a "360-degree profile" of an individual. By keeping data separate, the government, prevents the creation of a surveillance "master key" that could track a person's every movement.

4. Strict Penalties & Grievance Redressal (The Punishment)

   A law without consequences is just a suggestion.

   The DPDP Act, 2023 introduced significant financial penalties for non-compliance. If a Data Fiduciary doesn't take proper security measure to stop a Data Breach up to ₹250 Crore. Moreover, it gives citizen the right to have their complaint addressed, letting them take legal action to remove their data once the reason for collecting is no longer needed, which is also known as the "Right to be Forgotten".

   High penalties serve as a "Risk-Management" incentive. When the cost of a data leaked reaches the cost of hundreds of crores, organisation will choose to invest in the best encryption rather than taking risk.

5. Independent Regulatory Authority (The Watchdog)

   The state cannot decide whether its action are right or wrong.

   The Data Protection Board of India (DPB) is established under the DPDP Act. The

ISSN: 2582-6433

UIDAI manage the ID system, while the DPB acts as an independent referee that monitors everyone including the UIDAI itself. It has the authority of a civil court to call officials and require investigation.

Having an independent board means that if the government goes beyond its proper role, there's a fair and unbiased legal group that can step in and correct things. It provides a "Check and Balance" system that is essential in any democracy.

6. Technical Safeguard: Virtual IDs & offline Verification.

   We need to use advanced coding to protect biological data.

   Virtual ID (VID): Instead of sharing your permanent 12-digit Aadhar number you can generate a temporary, revocable 16-digit VID, A secure QR code helps to reduce the chances of "Authentication Failure" and data leaks by allowing offline verification. This helps to mask your real identity during transaction. This lets a store or bank check your identity right there using a signed digital code, without even linking to the main internet database.

   These tools help separate the main database from everyday use even if local store is hacked, they only have temporary VID or QR code scan, not your main biometric identity.

Conclusion

Biometric identity began as a tool for control. In history, biometric technique like fingerprinting were not developed to assist people: instead, they were created by colonial power to monitor, categorize, and manage indigenous population. For the British, the body become a means to track individual, especially those deemed criminal, and to sustain their authority. It is important to remember that this technology has "control" build into its core.

At present, the focus is on development and governance, today the aim has changed. In modern India, biometric like Aadhar are used for empowerment and welfare. This helps the government send food and money directly to the poor, cutting out corrupt middlemen. It also promote inclusion by giving million of people their first ever legal identity, allowing them to participate in modern economy. Additionally it improves efficiency by enabling digital bank accounts, SIM cards, and paperless services.

The risk of misuse is still there. However, because the system is a mix of different parts, we

ISSN: 2582-6433

cant ignore the possible dangers. As shown in cases like Tribune leak from 2018, centralized database are not very strong. A permanent threat: you can change your password, but you cant change your eyes or your fingerprint. A leak today can be a big problem for safety Surveillance: if there are no strong rules and no fair group watching over thing, there is always a chance that "government" might turn into "control," where the government uses data to follow every move people make.

Technology is a servant not a master. Aadhar is a powerful tool for development but it needs to be protected by the "Shield of Law," which includes the Puttaswamy judgment and DPDP Act. To be a truly modern democracy, India must ensure that a citizen's digital identity is used to open doors for them, not to build walls around them. The transition from being a "Colonial Subject" to becoming a "Digital Citizen" can only be successful I the citizen's privacy and dignity are at the core of the system.

References.

Fingerprint technique and its unique Bengal connection
https://www.livehistoryindia.com/story/eras/fingerprinting-technique
Sir Edward Henry's Classification and Uses of Finger Prints (1905) * Source Details: The original forensic manual showcasing the Bengal-born fingerprint indexing system.
Link: https://archive.org/details/b21463402
The PRS Legislative Research Statutory Mirror https://prsindia.org/billtrack/the-criminal-procedure-identification-bill-2022
The Law Enforcement Standard Operating Profile: State Crime Records Bureau (SCRB), System Mechanics and Operations of the National Automated Fingerprint Identification System, Madhya Pradesh Police, https://scrb.mppolice.gov.in/nafis.php
The Primary Enacted Legislation:The Criminal Procedure (Identification) Act, 2022, No. 11, Acts of Parliament, 2022 (India), available at Ministry of Home Affairs, https://www.mha.gov.in/sites/default/files/2022-11/CriminalPro_14112022%5B1%5D.pdf
The Analysis of Court Debates on Mass Surveillance (LiveLaw) * Source Details: A public, step-by-step documentation of the legal arguments regarding how a centralized identity database can facilitate a passive surveillance state Open Access Link:https://www.livelaw.in/aadhaar-hearing-weeks-2-3-petitioners-case-detail
Welfare Exclusion and Biometric Failure Study (Dr. Reetika Khera, 2017) * Source Details: The empirical study detailing how "biometric wear-and-tear" on manual laborers causes

ISSN: 2582-6433

fingerprint mismatches, leading to denial of food grains.

Open Access Link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102377

Aadhaar Failures and Food Security Denials (EPW Engage, 2019) * Source Details: A completely free, subscription-free public column hosted by the Economic and Political Weekly addressing technological transaction failures in rural sectors Open Access Linkhttps://www.epw.in/engage/article/aadhaar-failures-food-services-welfare

The Reality of Welfare Exclusion Post-Judgment (Scroll.in) * Source Details: An in-depth investigative article examining the physical exclusion rates of marginalized individuals due to system and network mismatch errors. Open Access Link:https://scroll.in/article/895966/the-daily-fix-in-its-aadhaar-judgment-the-court-shows-a-tendency-to-unsee-the-problem-of-exclusion

UK Parliamentary Research Briefing on Biometric Data: This official, public guide explains how the UK legal system defines and restricts the use of face and finger scans: https://researchbriefings.files.parliament.uk/documents/POST-PN-0731/POST-PN-0731.pdf

The Scrapping of the UK National ID Cards (The Guardian): A free-to-read, historical news article showing why the UK government decided to destroy its central identity database to protect civil rightshttps://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards

Analysis of China's Information Control Regime (Observer Research Foundation): A very clear and easy-to-read public study explaining how China uses cameras and databases to monitor public behavior:https://www.orfonline.org/expert-speak/china-s-social-credit-system-and-information-control-regime

The Aadhaar Constitutional Bench Judgment (Indian Kanoon): A free, public-access page containing the full legal verdict where Indian judges protected citizens' rights by banning private corporations from demanding Aadhaar scans :https://indiankanoon.org/doc/127517806/

This is the official public portal page explaining the creation of the Unique Identification Authority of India (UIDAI), its history under the Planning Commission, and its administrative role.

Source: Unique Identification Authority of India (UIDAI) - Organizational Structure.

StablePublicLink:https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html

This is the official release from the Press Information Bureau (PIB) of India. It details how the biometric identity system is used as an administrative tool to eliminate intermediaries, plug

ISSN: 2582-6433

leakages, and send welfare benefits directly to citizens' accounts.

Source: Press Information Bureau (PIB) - Direct Benefit Transfer (DBT) Progress Report.

StablePublicLinkhttps://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1576407&reg=3&lang=2

Nandan Nilekani's Official World Bank Team ProfileWhat is hosted here: The official biographical archive of Nandan Nilekani, detailing his transition from Co-founder of Infosys to employee #1 and first Chairman of the UIDAI.

Public Access Linkhttps://blogs.worldbank.org/en/team/n/nandan-nilekani

Nandan Nilekani's Official World Bank Team Profile

What is hosted here: The official biographical archive of Nandan Nilekani, detailing his transition from Co-founder of Infosys to employee #1 and first Chairman of the UIDAI.Public Access Linkhttps://cis-india.org/internet-governance/news/financial-express-november-20-2017-government-websites-made-aadhaar-details-public

Official UIDAI Explanation of Virtual ID (VID) and Privacy Tools: https://uidai.gov.in/en/contact-support/have-any-question/284-english-uk/faqs/aadhaar-online-services/virtual-id-vid.html